Question
Jukka Pitkänen · Mar 21, 2022

HMAC authentication problem

Hi! I'm banging my head to the wall with HMAC authentication. I have tried to implement this various ways but nothing seems to work.

If someone could help on this it would be great!

Here is a code that I have tried and working Javascript example, tested on Postman.

```
Set Appid = "itsasecretid"
Set Appkey = "itsasecretkey"
Set requestTimeStamp = $ZDATETIME($HOROLOG,-2)
Set nonce = ..getRandomString()
Set signatureRawdata = AppidrequestTimeStampnonce

Set keyUTF8 = $zconvert(Appkey,"O","UTF8")
Set signatureRawdataUTF8 = $zconvert(signatureRawdata,"O","UTF8")

Set tSigningKey = $SYSTEM.Encryption.HMACSHA(256, signatureRawdataUTF8, keyUTF8)
Set tSignature = ##class(%xsd.hexBinary).LogicalToXSD(tSigningKey)

//Set tSignatureBase64 = ##Class(%SYSTEM.Encryption).Base64Encode(tSigningKey)

Set tohmac = "hmac "Appid":"tSignature":"nonce":"requestTimeStamp
```

Javascript:

```
var crypto = require('crypto-js');
var APPId = "itsasecretid";
var APIKey = "itsasecretkey";
var time = (new Date()).getTime();
var times = Math.floor(time / 1000);
pm.environment.set("timestamp", times);
var nonce = getRandomString();
pm.environment.set("nonce", nonce);

var rawData = APPId + times + nonce;

var signature = CryptoJS.enc.Utf8.parse(rawData);
var secretByteArray = CryptoJS.enc.Base64.parse(APIKey);
var signatureBytes = CryptoJS.HmacSHA256(signature, secretByteArray)

var requestSignatureBase64String = CryptoJS.enc.Base64.stringify(signatureBytes);
var tohmac = "hmac " + APPId + ":" + requestSignatureBase64String + ":" + nonce + ":" + times;
```

#Authentication #Encryption #InterSystems IRIS
Product version: IRIS 2021.2